

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

United States of America
v.

Vitalii Antonenko

Case No.

19-MJ-4153 (DHH)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 2014 through January 2016 in the county of Middlesex in the District of Massachusetts, the defendant(s) violated:

Code Section 18 USC 1956(h) Offense Description (money laundering conspiracy)

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT OF SENIOR SPECIAL AGENT PETER GANNON

Continued on the attached sheet.

Peter J. Gannon
Complainant's signature

Special Agent Peter Gannon, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: 02/26/2019

City and state: Boston, Massachusetts

David H. Hennessy
Judge's signature



Hon. David H. Hennessy, Chief U.S.M.J.
Printed name and title

Criminal Case Cover Sheet

U.S. District Court - District of Massachusetts

Place of Offense: _____ Category No. II Investigating Agency USSS

City Cambridge

Related Case Information:

County Middlesex

Superseding Ind./ Inf. _____ Case No. _____
Same Defendant _____ New Defendant _____
Magistrate Judge Case Number _____
Search Warrant Case Number 16-MJ-4027 (DHH)
R 20/R 40 from District of _____

Defendant Information:

Defendant Name Vitalii Antonenko Juvenile: Yes No

Is this person an attorney and/or a member of any state/federal bar: Yes No

Alias Name _____

Address (City & State) New York City, NY

Birth date (Yr only): 1991 SSN (last4#): 0901 Sex M Race: W Nationality: USA

Defense Counsel if known: N/A Address N/A

Bar Number N/A

U.S. Attorney Information:

AUSA Seth B. Kosto Bar Number if applicable 641044

Interpreter: Yes No List language and/or dialect: Ukrainian

Victims: Yes No If yes, are there multiple crime victims under 18 USC§3771(d)(2) Yes No

Matter to be SEALED: Yes No

Warrant Requested Regular Process In Custody

Location Status:

Arrest Date _____

Already in Federal Custody as of _____ in _____

Already in State Custody at _____ Serving Sentence Awaiting Trial

On Pretrial Release: Ordered by: _____ on _____

Charging Document: Complaint Information Indictment

Total # of Counts: Petty Misdemeanor Felony 2

Continue on Page 2 for Entry of U.S.C. Citations

I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.

Date: 02/26/2019 Signature of AUSA: /s/Seth B. Kosto

District Court Case Number (To be filled in by deputy clerk): _____

Name of Defendant Vitali Antonenko

U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	<u>18 USC 1956(h)</u>	<u>money laundering conspiracy</u>	<u></u>
Set 2	<u></u>	<u></u>	<u></u>
Set 3	<u></u>	<u></u>	<u></u>
Set 4	<u></u>	<u></u>	<u></u>
Set 5	<u></u>	<u></u>	<u></u>
Set 6	<u></u>	<u></u>	<u></u>
Set 7	<u></u>	<u></u>	<u></u>
Set 8	<u></u>	<u></u>	<u></u>
Set 9	<u></u>	<u></u>	<u></u>
Set 10	<u></u>	<u></u>	<u></u>
Set 11	<u></u>	<u></u>	<u></u>
Set 12	<u></u>	<u></u>	<u></u>
Set 13	<u></u>	<u></u>	<u></u>
Set 14	<u></u>	<u></u>	<u></u>
Set 15	<u></u>	<u></u>	<u></u>

ADDITIONAL INFORMATION: _____

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Peter Gannon, being duly sworn, state as follows:

1. I am a Senior Special Agent with the United States Secret Service (“USSS”) and have been so employed since 1995. I received formal training at the Federal Law Enforcement Training Center (“FLETC”) in Glynco, Georgia and at the USSS Academy in Beltsville, Maryland. I am currently assigned to the FBI’s Joint Terrorism Task Force. My prior assignments, however, have included investigating violations of Title 18, United States Code, Sections 371 (conspiracy), 1028 (identity theft), 1028A (aggravated identity theft), 1029 (access device fraud), 1030 (computer fraud and abuse), 1341 (mail fraud), 1343 (wire fraud), 1344 (bank fraud) and 1956 (money laundering) on the Internet. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit these and other crimes.

2. I submit this affidavit in support of an application for a criminal complaint charging Vitalii Antonenko, with money laundering conspiracy, contrary to Title 18, United States Code, Section 1956(a)(1)(B) and in violation of Title 18, United States Code, Section 1956(h).

3. This affidavit is based on my personal participation in the investigation, as well as on information provided to me by law enforcement agents assisting in this investigation as described herein. This affidavit is being submitted for the limited purpose of establishing probable cause to secure a criminal complaint and arrest warrant. It does not set forth all the information gathered during this investigation.

Overview

4. At all times relevant to this affidavit:

a. Antonenko resided in New York City. Born in Ukraine, Antonenko became a naturalized U.S. citizen on August 1, 2014, during the course of the events described below. Antonenko controlled the e-mail account antvital@gmail.com.

b. Person 1 resided in or near Los Angeles, California, where Person 1 ran an unlicensed business that exchanged Bitcoin, a digital currency, for cash, and cash for Bitcoin.

c. Person 2 was an associate of Antonenko, who resided in New York City. Beginning in May 2015, Person 2 held a Bank of America checking account numbered xxxx-xxxx-7462. In connection with opening that account, Person 2 claimed to be unemployed.

5. Based on the investigation to date, and for the reasons set forth below, there is probable cause to believe that between at least March 2014 and approximately January 2016, Antonenko: (1) received Bitcoin constituting criminal proceeds from the online sale of stolen payment card data and personally identifiable information (“PII”); and (2) agreed to engage, and engaged, in Bitcoin-for-cash transactions with Person 1, Person 2, and others, intending both to conceal and disguise the nature and source of those criminal proceeds and to avoid federal transaction reporting requirements.

The Statutes

6. Title 18, United States Code, Section 1956(a)(1)(B) provides, in pertinent part:

(a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts ... such a financial transaction which in fact involves the proceeds of specified unlawful activity— ...

(B) knowing that the transaction is designed in whole or in part—

- (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
- (ii) to avoid a transaction reporting requirement

shall be sentenced to a fine of not more than \$500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years or both.

7. Title 18, United States Code, Section 1956(h) provides, in pertinent part that “any person who conspires to commit any offense defined in this section ... shall be subject to the same penalties as those prescribed for the offense of the commission of which was the object of the conspiracy.”

Investigation into “Website A”

8. The USSS is currently investigating one or more individuals (whose identities are unknown) for stealing and selling payment cards and the PII of U.S. citizens, to include names, dates of birth, and Social Security Numbers, all in violation of 18 U.S.C. §§ 1028 (identity fraud), 1028A (aggravated identity theft), 1029 (access device fraud), 1030 (computer fraud and abuse), and 1343 (wire fraud), as well as conspiracies to commit these offenses under 18 U.S.C. §§ 371 and/or 1349 (collectively “the Target Offenses”).

9. The unknown subjects offer the stolen payment card and PII data for sale on several black market “carding” websites, including, since at least as early as 2012, on Website A.

10. Since June 2015, law enforcement personnel acting in an undercover capacity from inside Massachusetts (“UC”) have purchased approximately 450 individuals’ PII or payment card information from Website A.

11. Specifically,

- a. On June 1, 2015, UC purchased the PII and payment card data of an account holder from California for approximately \$15 in Bitcoin.

- b. On January 20, 2016, UC purchased PII and payment card data for 46 American Express and 207 Mastercard accountholders for approximately \$1,550 in Bitcoin.
- c. On December 2, 2016, UC purchased PII and payment card data for 50 American Express accountholders from Massachusetts for approximately \$200 in Bitcoin.
- d. On June 2, 2017, UC purchased PII and payment card data for 50 American Express accountholders from Massachusetts for approximately \$200 in Bitcoin.
- e. On July 31, 2017, UC purchased PII and payment card data for 50 American Express accountholders from Massachusetts for approximately \$240 in Bitcoin.
- f. On September 25, 2017, UC purchased PII and payment card data for 50 American Express accountholders from Massachusetts for approximately \$225 in Bitcoin.

12. Based on my training and experience investigating online crimes and the fact there is no lawful way to sell third parties' PII and payment card information, the operators of Website A did not have authorization to distribute these victims' PII or payment card information.

13. There is accordingly probable cause to believe that Website A operates in furtherance of the Target Offenses, each of which is "specified unlawful activity" within the meaning of 18 U.S.C. § 1956(a)(1). *See* 18 U.S.C. § 1956(c)(7).

Tracing the Proceeds of UC's Transactions at Website A

14. According to the blockchain—a public register of all transactions conducted in Bitcoin—Website A accepted UC's June 2015 undercover payment at Bitcoin address 1Bheq4MispbRQu3ZBkmVKsA7Nth4yVYU4F (“the 1Bheq Address”).

15. Analysis of the 1Bheq Address and other Bitcoin transactions in the blockchain reveals that the 1Bheq Address is part of a cluster of addresses (sometimes referred to as a Bitcoin “wallet”) that contains approximately 19,000 related Bitcoin addresses (collectively “Wallet A”). The 19,000 payment addresses in Wallet A share common features, including control of encryption keys, that make it likely the addresses in Wallet A are controlled by the same persons or persons.

16. Analytical tools and discussions with other law enforcement officials with expertise in cybercrime reveal that Wallet A appears to contain one main group of addresses used by the operator of Website A to receive funds provided at signup for Website A accounts and to receive payment for purchases made at Website A, including the payment that UC made in June 2015.

17. According to the blockchain, Wallet A, which was active between November 2013 and July 2017, engaged in more than 575,000 separate Bitcoin transactions. Wallet A has both received and distributed approximately \$23 million.

Other Wallets Associated with the Operation of Website A

18. A significant percentage of the Bitcoin sent to Wallet A was forwarded to a second wallet (“Intermediary Wallet A”). More specifically, of the approximately 66,000 Bitcoin received by Wallet A since its creation, approximately 58,000 of that Bitcoin (almost 88 percent) went from Wallet A to Intermediary Wallet A.

19. Notably, UC's next transactions—in December 2015, January 2016, June 2017, and September 2017—all went to Bitcoin addresses associated with another wallet described here as

Wallet B. Wallet B, active since June 2015, has been associated with more than 1.5 million known transactions totaling approximately \$71,000,000.

20. Wallet B, in turn, sent more than \$20 million in the nine months between June 2015 and February 2016 to Intermediary Wallet A—the same wallet that received approximately 88 percent of the money sent to Wallet A.

21. These additional Bitcoin transfers to Intermediary Wallet A provide additional cause to believe that moneys directed to Intermediary Wallet A are proceeds from the operation of Website A, which is operated in furtherance of the Target Offenses.

Antonenko's Financial Links to Criminal Carding

Liberty Reserve

22. On October 17, 2012, using the gmail account antvital[at]gmail.com, Antonenko registered an account in his name and November 1991 date of birth at Liberty Reserve.

23. Before it was shuttered in May 2013 in connection with a criminal money laundering investigation brought by the U.S. Department of Justice and the U.S. Attorney's Office for the Southern District of New York, Liberty Reserve was one of the principal money transmitting services used by cybercriminals around the world to amass, distribute, store, and launder the proceeds of their illegal activity, including proceeds of investment fraud, credit card fraud, identify theft and computer hacking. As of May 2013, it had more than 5 million user accounts worldwide, including more than 600,000 accounts associated with users in the United States, and had processed millions of transactions. The site's founder admitted in his plea agreement to laundering more than \$250 million in criminal proceeds.

24. According to records obtained in connection with the Liberty Reserve investigation, between October 2012 and February 2013, Antonenko received approximately \$15,539 in payments from a Liberty Reserve account in the name of ValidShop.

25. At that time, ValidShop was an online criminal carding forum that sold stolen payment card data. Based on my training and experience and the training and experience of other USSS investigators, I am aware that criminal carding forums generally make payments to suppliers of services or inventory (i.e., stolen payment cards), not to customers of such sites. Additionally, there was no known legitimate business being conducted on ValidShop.

26. Between October 2012 and May 2013, a different Liberty Reserve account in the name “ferum511mac” made approximately \$51,651 in payments to Antonenko’s Liberty Reserve account.

27. At the time, “Ferum” was another known online criminal forum that sold stolen payment card data.

28. Again, investigators are not aware of any lawful reason for Antonenko or anyone else to be receiving payment in these total amounts from Ferum.

Bitcoin Payments to Antonenko

29. In connection with its investigation of Antonenko, USSS investigators used the blockchain to analyze three Bitcoin wallets associated with Antonenko.

30. Two of these wallets, numbered 12XtErsC78w3gzMZ7mYnsXub27FpQVTbDo (“the 12Xt Wallet”) and 1NkfRyNvALWrwXPD2VZM8A34UvEqWT78 (“the 1Nkf Wallet”), received transaction confirmations at Antonenko’s e-mail address antvital[at]gmail.com.

31. A third wallet associated with Antonenko, numbered 1GVF2dsMkCVUbjvFJdkJfFMXcLtHEV7M (“the 1GVF Wallet”), received incoming Bitcoin transactions from both the 1NkfR and 12Xt Wallets and from Intermediary Wallet A, and sent Bitcoin both to Person 1 (as described below) and to an account at BTC-e—a registered Bitcoin exchange—in Antonenko’s name.

32. As set forth in the table below, these three wallets associated with Antonenko sent and received significant amounts of Bitcoin between September 2013 and May 2017:

Wallet	Start Date	End Date	Amount ¹
1GVF	September 2013	March 2014	\$230,000
12Xt	November 2013	January 2014	\$40,000
1Nkf	March 2014	May 2017	\$465,000

33. More than \$140,000 of the amounts in the table above were transferred from either Wallet A or Intermediary Wallet A, the Bitcoin wallets described above that the investigation has associated with the operation of Website A and the Target Offenses.

34. Antonenko had no identified source of income that would account for these large-dollar Bitcoin transfers to and from wallets that he controlled, or for substantial cash deposits into traditional bank accounts that he held during this period.

35. According to records obtained from the Internal Revenue Service, for the tax years 2013 through 2016, inclusive, Antonenko was claimed as a dependent on a relative's tax return. That relative reported no more than \$38,000 in total income in any of those years. Antonenko himself filed no tax returns during these tax years, and tax transcripts show no employers reporting W-2 or 1099 payments to Antonenko that would explain the Bitcoin-for-cash activities described below.

¹ These amounts approximate the total amount of Bitcoin flowing through each wallet. A dollar both sent and received from the same wallet would thus be reflected as \$2, and if sent on to a second wallet, would be reflected in more than one row of this table.

36. Moreover, and as set forth below, beginning in January 2014 and continuing through January 2016, Antonenko regularly and immediately transferred Bitcoin he received from Wallet A and Intermediary Wallet A to the Bitcoin exchanger identified here as Person 1.

37. Person 1, in turn and in exchange for those Bitcoin, either gave Antonenko U.S. currency in person or deposited corresponding U.S. dollar amounts into bank accounts belonging to Antonenko and Person 2, among others.

38. Person 1 was not a money transmitter registered with the Treasury Department and its Financial Crimes Enforcement Network (“FinCEN”), which issue regulations aimed at deterring money laundering by requiring legitimate money remitters to both register with FinCEN and to obtain and keep records regarding their customers’ identities. Operating a money transmitting business without following FinCEN’s registration requirements violates Title 18, United States Code, Section 1960.

39. Through my review of certain of Person 1’s diary and financial ledgers—seized from Person 1 in connection with a separate criminal investigation in which she was ultimately charged²—I am aware that Person 1 purchased Bitcoin from Antonenko at a 9 to 10 percent discount below the prevailing market price for Bitcoin on Bitstamp, a currency exchange that is registered with FinCEN and does comply with its anti-money laundering regulations.

40. For example, Person 1 wrote in a diary of his/her activities on January 14, 2014:

I love that I’ve been buying from Vitali all week and he has more! I love that it’s been working out great. I love selling for 5-10% above [B]itstamp and buying for 9% below and making \$400 a day or more.

² Person 1 pleaded guilty in the United States District Court for the Central District of California to one count of operating an unlicensed money transmitting business and one count of money laundering in July 2018. Person 1 was later sentenced to a term of imprisonment.

41. On January 26, 2014, Person 1 wrote: “I love that I’m coming back to bitcoin trades. I love that I’m going to sell the shit out of these bitcoins that I lose money on and it’s all going to be ok because I’ll get cheap bitcoins from Vitali tomorrow.”

42. On July 9, 2014, Person 1 wrote “I love that Vitalii just sent me 2 coins! Woohoo! And I sent him money immediately. I love that he sends me coins and I have plenty of money in BofA so I can easily get him money.”

43. Person 1’s financial ledger similarly indicates in a column labeled “% from Bstmp” that Person 1’s transactions with Antonenko were priced at “-9.0%” to the prevailing Bitstamp price.

44. Based on my training and experience as a financial investigator, and based on my conversations with investigators and analysts familiar with cryptocurrency markets, I am aware that a 9 percent discount below a publicly available sale price for Bitcoin is a standard rate for unlicensed money remitters, who in exchange for that discount are offering their customers the ability to avoid having to provide traceable identifying information that would be required in market rate transactions.

45. Antonenko’s consistent use of an unlicensed exchanger provides additional cause to believe that he is laundering Bitcoin proceeds that he received from the operators of Website A. (As noted above, there is probable cause to believe that moneys Antonenko received from the operators of criminal carding forums are proceeds of the Target Offenses). Based on my training and experience as a financial investigator, there is no legitimate reason for Antonenko to have sold Bitcoin at a below-market price to Person 1 unless he was attempting to conceal the unlawful source of the Bitcoin.

46. The mechanism that Person 1 used to return the proceeds of these Bitcoin transactions to Antonenko—making structured cash and other deposits into the bank of accounts of Antonenko and Person 2—reinforces my belief that Antonenko and Person 1 are engaging in financial transactions involving the proceeds of the Target Offenses with the intent to conceal the source of the funds and avoid reporting requirements.

47. Presented below are several examples of financial transactions that move serially from the Website A-linked Intermediary Wallet A, to one of Antonenko's Bitcoin wallets, to Person 1's Bitcoin wallet, to the bank accounts of Antonenko or Person 2.

48. On March 30, 2014, at 7:37 p.m., Intermediary Wallet A sent Antonenko's 1Nkf Wallet 25 Bitcoin. On April 1, 2014, in his next Bitcoin transaction from the same wallet, Antonenko forwarded 24.9999 Bitcoin to Person 1's wallet.

49. Person 1's ledger for April 1, 2014 shows "24.9999" in "BTC", an "\$11,033" entry under the name Vitalii and the notations "Citibank" and "-9.0%" from "Bstmp." Based on my training and experience as a financial investigator and the investigation to date, I interpret the ledger to record a transaction in which Person 1 purchased 24.9999 Bitcoin from Antonenko for \$11,033. Person 1 noted the purchase of the Bitcoin at a 9 percent discount from the prevailing price on the Bitstamp exchange.³

50. Citibank records for a joint account in the names of Antonenko (numbered xxxxxx4370) and a relative show two cash deposits on consecutive days totaling exactly \$11,033. The first deposit, on April 1, 2014—the same day Antonenko's wallet sent Bitcoin to Person 1's

³Based on the price that Person 1 recorded—nine percent below Bitstamp—I would expect that the amount of currency Antonenko received in exchange for his Bitcoin would be approximately 9 percent less than the value of the Bitcoin he sent to Person 1. I attribute any variance from this amount to the fact that Bitcoin's market price fluctuates.

wallet—was for \$9,900 at a Citibank branch in California, where Person 1 resides (and where Antonenko and his relative did not). A second deposit, on the next day (April 2, 2014), was for \$1,133 at a different Los Angeles-area Citibank branch. As noted above, these two deposits in Citibank’s records match Person 1’s ledger exactly, which causes me to believe that Person 1 made or directed these two cash deposits.

51. There are two features to these April 1 and April 2 deposits that cause me to believe that Antonenko and Person 1 were attempting to conceal the source of the funds for them. First, Person 1 deposited \$9,900 into Antonenko’s account on April 1, 2014. This amount is just \$100 below the threshold that would require Citibank to generate a Currency Transaction Report (“CTR”) to FinCEN for a cash transaction involving \$10,000 or more. Based on my training and experience investigating financial frauds, engaging in cash transactions just below the CTR threshold is indicative of intent to evade the CTR requirement, which itself can be a violation of federal criminal law. *See* 31 U.S.C. § 5324.

52. Second, Person 1 and Citibank’s records indicate that Person 1 split the \$11,033 payment to Antonenko across two days, again evidencing an intent to disguise the true (i.e., over \$10,000 in cash) nature of Person 1’s payment to Antonenko. That Person 1 directed these deposits at two different Los Angeles area Citibank branches only provides further indicia of an intent to disguise the true nature of the transaction from Citibank and from the investigators who rely on CTRs.

53. In a second group of serial transactions, on April 11, 2014, Intermediary Wallet A sent 26.25 Bitcoin (valued at approximately \$10,579.28) to Antonenko’s 1Nkf Wallet. The same day, Antonenko forwarded 26.2 Bitcoin to Person 1’s wallet. Person 1’s payment ledger shows a payment that day to “Vitalii” totaling “\$10,109” for “26.2” Bitcoin.

54. Citibank's record of Antonenko's account shows two separate deposits that same day at different Los Angeles area branches: a \$7,609 cash deposit at one Citibank branch and a \$2,000 cash deposit at a second. These deposits total \$9,609, exactly \$500 less than the amount reflected in Person 1's ledger, and just below the \$10,000 CTR threshold. Based on other instances described above of Person 1 making deposits that evidence an intent to skirt the CTR threshold, these April 11, 2014 transactions cause me to believe that Antonenko and Person 1 were attempting to avoid reporting requirements and conceal the origin of the funds Person 1 was depositing into Antonenko's Citibank account by keeping the deposit amount just below \$10,000.

55. On May 20, 2014, Person 1 and Antonenko engaged in another series of transactions involving Bitcoin that arrived from the Website A-related wallet. At 11:39 a.m., Intermediary Wallet A sent 8.65 Bitcoin (valued at approximately \$4,018.10) to Antonenko's Bitcoin wallet. That same day, Antonenko forwarded 8.5 Bitcoin to Person 1. Person 1's ledger reflects that later that day, a \$3,790 entry appears under the name "Vitalii" and the notation "Citibank" in connection with the purchase of "8.5" Bitcoin. Citibank records, in turn, show a \$3,790 cash deposit into a Citibank branch in Granada Hills, California. Person 1's records also indicate that Person 1 later re-sold the Bitcoin that s/he received from Antonenko at an approximately 10 percent profit (*i.e.*, at or above market price).

56. On July 5, 2014, Person 1 and Antonenko engaged in another series of transactions involving Bitcoin that arrived from the Website A-related wallet. At 6:42 p.m., Intermediary Wallet A sent 4 Bitcoin (valued at approximately \$2,669.41) to Antonenko's 1Nkf Wallet. At 7:35 p.m., less than an hour later, Antonenko's Bitcoin wallet forwarded 4 Bitcoin to Person 1's Bitcoin wallet. Person 1's financial ledger reflects a payment to "Vitalii" of "\$2,290" via "BofATransfer" for the sale of "4" Bitcoin.

57. Antonenko's Bank of America records for an account in his name ending in 0170 show an "Online Banking Transfer L [Person 1]" for the same amount, \$2,290.

58. On December 16, 2014, Person 1 and Antonenko engaged in another series of transactions involving Bitcoin that arrived from the Website A-related wallet. At 9:29 p.m., Intermediary Wallet A sent 6.2 Bitcoin (valued at approximately \$2,089.79) to Antonenko's 1Nkf Wallet. At the same approximate time, Antonenko forwarded 6.17 Bitcoin to Person 1. Person 1's payment ledger for that day reflects an entry for \$1,870 for the purchase of 6.17 Bitcoin under the name "Vitalii" and a notation "BofADeposit."

59. I have reviewed Bank of America records for the Antonenko account ending in xxxxxxxx0710, which show a deposit in the exact amount reflected in Person 1's ledger — \$1,870—at a branch in Santa Monica, California. This causes me to believe that Person 1 made or directed the deposit into Antonenko's Bank of America account, and that Person 1 learned directly or indirectly from Antonenko the account number needed to make the Bank of America deposit.

60. On December 26, 2014, Person 1 and Antonenko engaged in another series of transactions involving Bitcoin that arrived from the Website A-related wallet. At 3:53 p.m., Intermediary Wallet A sent 6.2 Bitcoin (valued at approximately \$2,008.86) to Antonenko's 1Nkf Wallet. At approximately 4:27 p.m., just over half an hour later, Antonenko forwarded 6.17 Bitcoin to Person 1. Person 1's payment ledger for that day reflects a \$1,814 payment to "Vitalii" for the purchase of 6.17 Bitcoin and a notation "BofADeposit."

61. Bank of America records show a deposit in the exact amount reflected in Person 1's ledger —\$1,814— into account number xxxxxxxx0170 at a branch in Van Nuys, California. This again causes me to believe that Person 1 made or directed the deposit of Website A-related funds into Antonenko's Bank of America account.

62. In one instance in 2014 identified to date, Antonenko's 1NKf Wallet took money directly from Wallet A, the same wallet that UC paid in June 2015 to purchase PII and payment card data from Website A. Specifically, on March 17, 2014, the 1NKf Wallet received 25 Bitcoin from Wallet A. The next day, March 18, 2014, Antonenko's 1GVF Wallet sent 15.17 Bitcoin to Person 1's wallet.

63. Person 1's ledger shows a March 18, 2014 purchase of 15.67 Bitcoin from "Vitalii" and a resulting deposit of \$8,690 into Antonenko's Citibank account. Antonenko's Citibank records reflect the \$8,690 deposit at a branch in Granada Hills, California.⁴

64. Overall for the calendar year 2014, Person 1's ledger shows that Person 1 paid Antonenko more than \$335,000 in cash and bank deposits. Not all of these amounts originated with wallets associated with the operation of Website A, but as noted above, there is probable cause to believe that the Website A-related amounts are the proceeds of illegal activity, and that Antonenko's use of Person 1 as an unregistered Bitcoin exchange was to conceal the origin of those funds, and to avoid the consequences of cash transactions in these amounts.

65. Although Person 1's digital ledger stops at the end of 2014, the pattern of payments continued well into 2015—from the Intermediary Wallet A, to Antonenko's Bitcoin wallet, to Person 1's Bitcoin wallet, to an Antonenko bank account through California-based branch deposits in a slightly lower amount—as reflected in the table below.

DATE	Intermediary Wallet A to Antonenko Wallet	Antonenko Wallet to Person 1 Wallet	California Deposit into Antonenko Bank
1/8/15	7.17 BTC (\$2,073.56)	7.17 BTC (\$2,073.56)	\$1,902

⁴The investigation has yet to reveal why Person 1's ledger shows a purchase from Antonenko of .5 Bitcoin more than Antonenko sent to Person 1's wallet—Antonenko sent 15.17 Bitcoin but is noted as having sold 15.67 Bitcoin. The transaction is nevertheless significant because it provides probable cause to believe that Antonenko used Person 1's covert services to convert Bitcoin that he received directly from Wallet A to cash.

3/9/15	3.63 BTC (\$1,025.66)	3.7 BTC (\$1,045.44)	\$953
4/20/15	4.88 BTC (\$1,096.54)	4.77717 BTC (\$1,073.43)	\$975
5/5/15	4.38 BTC \$1,035.83	3.717 BTC \$879.03	\$795
5/28/15	7.79 BTC (\$1,858.23)	7.7717 BTC \$1,853.86	\$1,357
6/8/15	10.38 BTC (\$2,353.87)	11.17 BTC (\$2,578.37)	\$2,320

66. Antonenko's bank statements also suggest that Person 1 (or a relative acting at her direction) continued to cause cash or direct deposits into the accounts of Antonenko or Person 2 well into 2017.

67. For example, Antonenko's November 2015 statement for a Wells Fargo account in his name numbered xxxxxxxx166 shows "Transfer[s] from [Person 1]" totaling approximately \$4,000. Throughout 2016 and as late as March 2017, Antonenko's Wells Fargo account also received approximately \$19,700 in transfers from an account in the name of Person 1's sister. Law enforcement personnel familiar with the investigation of Person 1 are aware that Person 1's sister participated in Person 1's unlicensed Bitcoin exchange business at Person 1's direction.

68. There is also probable cause to believe that Person 1 made cash deposits directly in to Person 2's Bank of America account.

69. Depicted below, for example, is surveillance video of Person 1 in Bank of America's Sepulveda-Sherman Banking Center making a \$7,000 cash deposit into Person 2's bank account on August 13, 2015.



70. On July 26, 2015, Antonenko sent 1.23 Bitcoin (valued at approximately \$358.52) to Person 1's wallet. Bank of America records for Person 2's account show a deposit the next day of nearly the same amount—\$328—at the same Sepulveda Sherman Banking Center. Based on the investigation to date and based on all of the transactions that Person 1 directed into Antonenko's accounts from the same banking center, there is probable cause to believe that Person 1 made or directed the July 27, 2015 deposit.

71. On December 22, 2015, at approximately 10:03 a.m., Person 2's Bank of America records show a \$965 cash deposit made at the same Sepulveda Sherman Banking Center. Notably, Wells Fargo records show a \$3,000 cash deposit into an account in Antonenko's name that took place less than 90 minutes later at Wells Fargo's 10225 Balboa Boulevard branch in Northridge, which is just over 6 miles from the Sepulveda Sherman Banking Center.

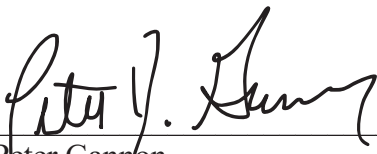
72. Based on the investigation to date and for all of the reasons described above, there is probable cause to believe that Person 1 made or directed both December 22, 2015 deposits, and that

the deposits were split across 2 different financial institutions and two account holders to conceal and disguise the nature of the Bitcoin-for-cash transactions.

Conclusion


73. For all of the reasons stated above, probable cause exists to believe that Vitalii Antonenko conspired with Person 1, Person 2, and others to violate 18 U.S.C. § 1956(a)(1)(B) in violation of 18 U.S.C. § 1956(h).

I swear to the foregoing under penalties of perjury.



Peter Gannon
Senior Special Agent
United States Secret Service

Sworn and subscribed to me this 26th day of February 2019



HONORABLE DAVID H. GUINNESS
UNITED STATES MAGISTRATE JUDGE

